CLERK'S OFFICE
A TRUE COPY
Nov 25, 2020
s/ Daryl Olszewski
Deputy Clerk, U.S. District Court
Eastern District of Wisconsin

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Information associated with the account listed on Attachment A that is stored at premises owned, maintained, controlled, or operated by Microsoft Corporation, an email and electronic services provider headquartered at One Microsoft Way, Redmond, WA 98052.

Case No. 20 MJ 255

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the _____ District of _____, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. Sections 1028, 1343,1344 and 1956	Fraud and related activity in connection with identification documents; Fraud by wire, radio, or television; Bank fraud; and Laundering of monetary instruments.

The application is based on these facts:

See attached affidavit.

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

DHS Special Agent John Cerf
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: November 25, 2020

Judge's signature

City and state: Milwaukee, WI.

Hon. William E. Duffin, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, John Cerf, being duly sworn, hereby depose and state that the following is true to the best of my information, knowledge, and belief:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the United States Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) since July 2008. I have been assigned to investigate financial crimes to include money laundering and fraud related offenses committed by criminal organizations. I have received specialized training in the enforcement of federal financial crime. I have also debriefed defendants and witnesses; conducted physical and electronic surveillance; executed arrest and search warrants; and analyzed evidence. My job responsibilities include investigating violations of federal law, including but not limited to financial crimes. As part of my assignments, I have received formal training from the Federal Law Enforcement Training Center, as well as training through experts from various law enforcement agencies.

2. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that are stored at premises controlled by Google, LLC, an email and electronic services provider headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043; Microsoft Corporation, an email and electronic services provider headquartered at One Microsoft Way, Redmond, WA 98052; and Oath Holdings, Inc., an email and electronic services provider headquartered at 701 First Avenue, Sunnyvale, CA 94089.

3. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google, LLC, Microsoft

Corporation, and Oath Holdings, Inc. to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

4. The information supplied in this affidavit is based upon my investigation as well as information provided and investigation conducted by other law enforcement personnel in this matter to date, all of which I consider reliable. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not set forth every fact related to, or otherwise the product, of this investigation.

5. The accounts to be searched are listed on Attachment A.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b) (1) (A), & (c) (1) (A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3) (A) (i).

RELEVANT STATUTES

7. This investigation concerns alleged violations of Title 18, United States Code, Section 1028, fraud and related activity in connection with identification documents; Section 1343, fraud by wire, radio, or television; Section 1344, bank fraud; and Section 1956, laundering of monetary instruments.

DEFINITIONS

8. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. The term "computer," as defined in 18 U.S.C. §1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

b. "Mobile computing devices," as used herein, are portable computers which have the capability to access the internet. Mobile computing devices include, but are not limited to, laptops, tablets and smartphones.

c. "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

d. "IP Address", as used herein refers to The Internet Protocol address, which is a unique numeric address used by computers on the Internet. An IP address looks like a series of numbers and/or characters often separated by periods or colons (e.g., 192.168.0.1 and 603:6000:db00:b400:6cfe:2ee0:3ced:c8be). Every device attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that device may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers and mobile computing devices have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

e. "Synthetic Identity" refers to a personal identity that may be completely fictitious or partially fictitious. A synthetic identity requires a name, date of birth, social security number, address, and phone number. Synthetic identities are typically created for nefarious

purposes and often involve counterfeit identification, which permits a real person to evade law enforcement or benefit from a fraud scheme.

f. "Shell Company" refers to a business, typically with formal registration, which lacks business operations or significant assets. Shell companies can be used to disguise illegal operations, evade law enforcement, or benefit from a fraud scheme.

g. "PayPal" is a peer to peer program that allows for the transfer of money, digitally and without fees, between PayPal accounts or accounts held across participating financial institutions. Upon registration with an e-mail or mobile phone number, PayPal can be operated on mobile computing devices to digitally send and receive money without appearing at a financial institution.

OVERVIEW AND BACKGROUND OF INVESTIGATION

9. This investigation of financial fraud relates to the use of synthetic identities and shell companies by Lee S. DAGOSTINI to promote the illicit transfer of money between various financial institutions and to facilitate illicit withdrawals to accomplish financial fraud, money laundering, and other criminal activities. The investigation has identified multiple synthetic identities and shell companies associated with addresses, telephone numbers, emails and IP addresses tied to DAGOSTINI. Many of the financial accounts opened with synthetic identities were opened with applications on the internet, which would allow DAGOSTINI to avoid appearing in person at the financial institutions. Counterfeit identification and a form of secondary identification, such as wage statements or utility bills, were provided to financial institutions upon request, in order to falsely confirm the applicant's identity. After the opening of a financial account in this manner, DAGOSTINI used the fraudulent financial account to make purchases, and to receive, send, and withdraw money obtained by way of the financial fraud. The synthetic identities

and shell companies identified to date, are all linked to Lee S. DAGOSTINI, the target of this investigation by overlapping personal identifiers. The email accounts identified in Attachment A were opened and linked to the synthetic identities as part of the alleged fraud scheme.

Creation of Synthetic Identities

10. When an individual undertakes to create a synthetic identity, he or she uses a name, date of birth, social security number, address, phone number, and possibly other information such as an email account, to create the profile of a fictitious person. Pieces of real identity information may combined with fictitious identity information. For example, the address for the synthetic identity is often real, while the name, date of birth, and social security number could be fictitious. In some cases, a synthetic identity may use personal identity information that is confusingly similar to an actual person's identity, as where a name, date of birth, or social security number is similar but just slightly different than those of a real person.

11. As with actual identities, a person presenting a synthetic identity as part of a financial fraud scheme will be required to provide proof of identity. Counterfeit identity documents are often obtained and used to support a synthetic identity. Common counterfeit identity documents include state driver's licenses and social security cards. Supplemental counterfeit documents such as utility bills and wage statements are also frequently used to support the association of a synthetic identity to an address within a recent time frame. Counterfeit identity documents can be purchased discretely from a vendor via the internet with a credit card payment.

12. Once a synthetic identity has been created, it can be used to apply for credit card and bank accounts. This can be accomplished electronically by using the internet to access a financial institution's website. This electronic process typically requires an email account. The email account

then provides a discreet method for the perpetrator to send and receive communications concerning accounts, including the means to supply proof of identity.

13. After a synthetic identity has an established credit or bank account, the person controlling it can use the account to make typical purchases for expenses such as fuel, groceries, restaurants, entertainment, and other services. Initially, those charges are paid in a timely manner to ensure that the synthetic identity develops a positive credit history.

14. After establishing a positive credit history, which may take months or even years, a person can use the synthetic identity to apply for new credit card accounts that provide a higher credit limit or request higher credit limits on existing accounts. The accounts can be used to commit financial fraud without repercussions to the individual who controls the synthetic identity. Financial fraud known as a "bust out" schemes happen when a credit account is used to reach or exceed the credit limit with no intention to make payment on the balance owed. To maximize the "bust out" scheme, the account may initially be paid, fully or partially, to acquire a higher credit limit, which later allows for a larger "bust out" scheme.

Dagostini's History

15. On December 1, 2005, Lee S. DAGOSTINI was convicted of financial fraud in federal court in the Eastern District of Wisconsin in case number 04-CR-146. The counts of conviction included possession of 15 or more unauthorized access devices, in violation of Title 18, United States Code, Section 1029(a)(3); mail fraud, in violation of Title 18, United States Code, Section 1341; money laundering, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i); and money laundering conspiracy while subject to release, in violation of Title 18, United States Code, Section 1956(h) and 3147. In the commission of these crimes, DAGOSTINI used 31 synthetic identities to obtain bank and credit card accounts and incur debts on those credit

card accounts without repaying them. DAGOSTINI used voicemail accounts, mail services, and shell companies to accomplish a bust out fraud scheme that put at risk more than $2,000,000 of financial institution funds. The scheme began in 1995 and continued into 2005, with DAGOSTINI surreptitiously continuing to execute it even while he was on pretrial release during the pendency of his federal case. On January 20, 2006, DAGOSTINI was sentenced to 151 months in prison, followed by 5 years of supervised release. He was also ordered to pay restitution of $1,216,557.64.

Dagostini's Actual Identifiers

16. Upon his 2014 release from prison, DAGOSTINI reported to U.S Probation Officer Andrea Schachtner for supervised release. He represented to her that his residence was located at 311 N Greenfield Avenue, Waukesha, WI 53186 ("**311 N Greenfield Ave**"). During his period of supervised release, which began in August 2014 and terminated on August 11, 2019, USPO Schachtner communicated with DAGOSTINI using the email addresses **leedago@gmail.com** and **Biztimenow@gmail.com**.

17. On July 15, 2019, DAGOSTINI provided this same residential address along with the phone number **414-940-9975**, and the email **leedago@gmail.com** on his financial statement to the Financial Litigation Unit ("FLU") of the United States Attorney's Office, Eastern District of Wisconsin ("USAO WIE"), in accordance with his post-supervision restitution agreement. As part of her oversight of that agreement, USAO FLU Agent Kim Camomilli has called, spoken to, and received phone calls and voice mail messages from DAGOSTINI via the phone number **414-940-9975** since July 2019.

18. Waukesha County property records reflect that the residence at **311 N Greenfield Ave** has been owned by Sandra Randall and Zachary Randall[1] since 2017. The property was

[1] Zachary Randall is believed to be Sandra Randall's son by a previous relationship.

previously owned by Sandra Randall's mother, Donna Zilbert, who DAGOSTINI listed as his emergency contact on his September 2019 U.S. Passport application. Although Waukesha County Circuit Court records reflect that Sandra Randall is DAGOSTINI's former wife, and that the two divorced on March 7, 2016, through recent surveillance of that location, I have confirmed that both DAGOSTINI and Sandra Randall currently occupy the residence at **311 N Greenfield Ave.**

19. I have also confirmed that DAGOSTINI drives vehicles that are registered to Sandra Randall at that address. On July 24, 2019, DAGOSTINI received a citation through the Waukesha City Municipal Court for a moving violation while driving a 2007 VW with Wisconsin registration plate 446VLU. Wisconsin Department of Transportation ("WIDOT") records indicate the vehicle is registered to Sandra M Randall at **311 N Greenfield Ave**. During surveillance in October 2020, agents also observed DAGOSTINI driving a black Mercedes Benz ML320, with Wisconsin Brewers style registration plate QVD25. This vehicle is also registered to Sandra M. Randall at **311 N Greenfield Ave.** Agents have seen both the 2007 VW and the black Mercedes, along with several other vehicles, regularly parked at the **311 N Greenfield Ave** location.

20. To confirm DAGOSTINI's actual identifiers, I have also reviewed numerous business and financial records that I have obtained in the course of this investigation. The records reflect the information contained in paragraphs 21-24.

21. U.S. Cellular records reflect that the telephone call number **414-940-9975** was activated with U. S. Cellular on February 2, 2017 as a prepaid account. Prepaid cellular accounts do not require complete customer registration information. The account name is recorded as Sam Doe and the associated email is listed as **leedago@gmail.com.** An email associated with a prepaid phone account allows a customer to log into the account via the internet and prepay for service. The email account **leedago@gmail.com** was linked to three mobile devices: Samsung Galaxy A20,

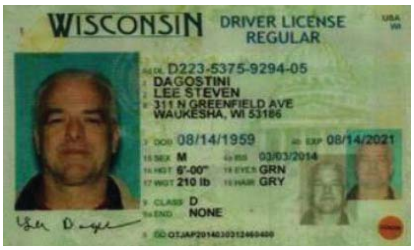
Samsung Galaxy J3 2017, and Nuu Mobile A6LC. Call history for **414-940-9975** shows outgoing calls to phone numbers associated with Sandra Dagostini, Savannah Dagostini, Badger Health Center, Landmark Credit Union, Prohealth Waukesha, Orthopedic Associates of WI, DHL Express, TransUnion, GTE Financial Credit Union, Fifth Third Bank, Equifax, and Summit Credit Union. Several of these numbers belong to DAGOSTINI family members and a number of others belong to financial institutions where the evidence shows that DAGOSTINI has established new accounts using synthetic identities.

22. I have also reviewed Google records that I have received to date. Those records reflect that the email address **leedago@gmail.com** was originally created March 25, 2011, and was registered in the name Lee DAGOSTINI. According to records received through June 12, 2020, the last login to the account up to that time was June 9, 2020. The account has a recovery email **Biztimenow@gmail.com** and a sign-in/recovery phone number **414-940-9975.** A recovery email and/or phone number are pieces of contact information provided by a customer to enable the customer to receive a temporary password if the account becomes locked or if a password is forgotten. Therefore, the customer must have access to the recovery email and phone that have been provided in order to make use of this feature.

23. The Google records further reflect that email account **Biztimenow@gmail.com** was created February 23, 2014, and was registered to the name Lee DAGOSTINI. The recovery email for the account is **leedago@gmail.com.** According to records received through June 29, 2020, the last login to the **Biztimenow@gmail.com** account up to that time was November 21, 2019.

24. I have also reviewed records provided by WIDOT. Those records reflect that WIDOT issued a driver's license to DAGOSTINI in the name Lee Steven DAGOSTINI, date of birth **08/14/1959,** with license number **D223-5375-9294-05**, and that on March 3, 2014, the address

for that license was updated to **311 N Greenfield Ave.** A copy of the updated license is set forth below.



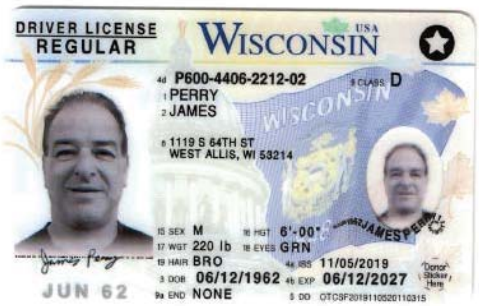
25. In September 2019, DAGOSTINI applied for a U.S. passport with an application that included the date of birth **08/14/1959**, the social security number **399-76-5139**, the address **311 N Greenfield Ave**, the phone number **414-940-9975**, and the email **leedago@gmail.com.** On the application, DAGOSTINI stated he had been married to Sandra Randall but divorced as of March 7, 2016. His emergency contact was listed as Donna Zilbert, identified as his mother-in-law, with an address of 6156 Kimberly Elise Dr., Bartlett, TN 38135. As proof of identity, he provided his Wisconsin driver's license with number, **D223-5375-9294-05**, and his birth certificate.

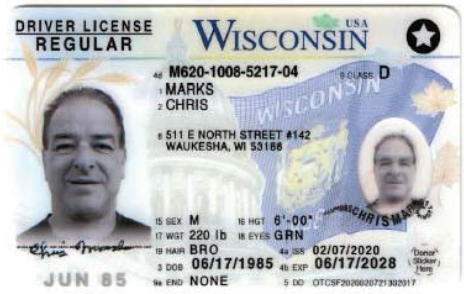
26. As is further developed in the paragraphs below, these confirmed actual identifiers for DAGOSTINI, that is, the address **311 N Greenfield Ave**, Waukesha, Wisconsin, the phone number **414-940-9975**, and the email addresses **leedago@gmail.com** and **Biztimenow@gmail.com** are all tied to the new fraud activity for which DAGOSTINI is currently under investigation.

The Current Investigation: Seizure of Counterfeit Identification Documents

27. On March 18, 2020, a Customs and Border Protection (CBP) officer assigned to the CBP Milwaukee office selected DHL international parcel 2433362956 for examination. The shipment was sent from Guangzhou Fan Xu Company LTD of Hong Kong and was addressed to

Steven DAGOSTINI [2]at **311 N Greenfield Ave**, Waukesha, WI. The package was declared as "synthetic hair." [3] The parcel contained a wig and three sets of counterfeit identity documents (six total) purporting to be Wisconsin driver's licenses. One set contained the name of *James PERRY,* [4] DL number P600-4406-2212-02, DOB 06/12/1962, and address 1119 South 64th Street, West Allis, WI 53214; one set contained the name *Chris MARKS*, DL number M620-1008-5217-04, DOB 06/17/1985, and address **511 E North Street, #142,** Waukesha, WI 53188; and one set contained the name *Dylan YATES*, DL number Y320-1606-9291-03 with DOB 08/11/1969, and address **511 E North Street, # 129,** Waukesha, WI 53188. All six contain DAGOSTINI's photo. WIDOT has no record of issuing Wisconsin driver's licenses in these names with these DL numbers. The documents were seized pursuant to Title 19, United States Code, Section 1595a(a), merchandise imported contrary to law, and Section 1584, false manifest. Copies of the documents are set forth below.





[2] All of the synthetic identities identified during this investigation are italicized throughout this affidavit.
[3] On February 18, 2020, a previous international parcel declared as synthetic hair was sent from Guangzhou Fan Xu Company LTD of Hong Kong to *Patrick Franke* at 311 N Greenfield Ave. This parcel was not examined by CBP and presumably was delivered to the intended destination. *Pat Franke* is a synthetic identity that DAGOSINI created as part of the fraud scheme for which he was convicted in Case No. 04-CR-146. Other details regarding the current use of the *Pat Franke* synthetic identity are further developed in the paragraphs herein.
[4] *James Perry* with a DOB 6/12/1962 is also a synthetic identity that DAGOSTINI created and used as part of his previous fraud case.

28. I have determined that the address of **511 E North Street, Waukesha, WI 53188** ("**511 E North St**"), which is on two sets of the counterfeit documents, is the location of North Shore Station, a commercial building which houses a laundromat, a mail and office service, and a tanning service. The mail service located inside the North Shore Station building is known as MailEx. Mailboxes are numbered 101 through 142 and are lockable with a key. A posting near the mailboxes explains that the service offers private mailboxes and that to be received at the facility, mail must contain both the building address and a specific box number (e.g. 511 E North St #101).

29. During surveillance conducted between June and October 2020, I and other agents observed that there were numerous occasions when DAGOSTINI traveled to **511 E North St**, entered the North Shore Station building, and exited after less than five minutes carrying what appeared to be mail matter.

30. On April 8, 2020, a CBP officer assigned to the CBP Milwaukee office made a second seizure of counterfeit documents. The officer had selected DHL international parcel 1010752260 for examination. The shipment was sent from Guangzhou Reputation Company LTD of Hong Kong to *Patrick FRANKE* at 741 N Grand Avenue #201, Waukesha, WI 53186 ("**741 N Grand Ave #201**"), phone **414-940-9975**. Again, the package was declared as "synthetic hair." The parcel contained a wig and three sets of counterfeit identity documents (six total) that were identical to the documents seized on March 18, 2020. That is, the parcel contained counterfeit Wisconsin

driver's licenses, two each in the names of *James PERRY,* license number P600-4406-2212-02, *Chris MARKS,* license number M620-1008-5217-04, and *Dylan YATES*, license number Y320-1606-9291-03, all bearing DAGOSTINI's photo. The documents were seized pursuant to Title 19, United States Code, Section 1595a(a), merchandise imported contrary to law, and Section 1584, false manifest.

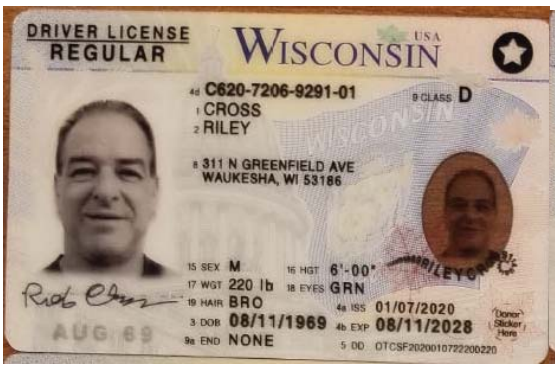
31. The building at the address on the seized parcel, **741 N Grand Avenue,** Waukesha, Wisconsin, is a commercial office building operated by Center City Plaza, LLP. The building directory indicates that Suite # 201 is occupied by Plac Associates. Documents obtained from Center City Plaza, LLP, reflect that Suite # 201 was leased on May 18, 2018 to *Patrick FRANKE* d.b.a. Plac Associates, described as a loan broker business, with a main address of **N51W34917 Wisconsin Avenue,** Okauchee, WI 53069,[5] phone number **414-940-9975,** and email **pfis12345a@gmail.com**. The lease lists the company principal as *Patrick FRANKE*, DOB 09/05/1969, with social security number 397-15-1696, and address **9949 W. Atlantic Blvd.**, Coral Springs, FL 33071. As noted in footnote 3 above, DAGOSTINI used the name *Pat FRANKE,* as an identifier for one of the synthetic identities he created in his prior fraud scheme, and *Patrick FRANKE* was the addressee on a previous package from Hong Kong in February 2020. Further details about the *Patrick FRANKE* synthetic identity are set forth in paragraphs below.

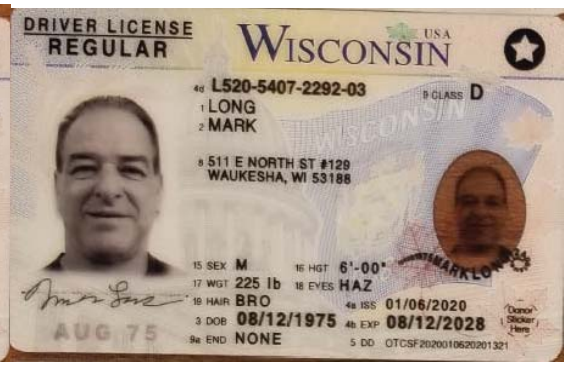
32. On August 11, 2020, another agent doing follow up investigation in this case conducted surveillance on DAGOSTINI and observed him depart from **311 N Greenfield Ave** driving the black Mercedes Benz ML 320. The agent followed DAGOSTINI to **741 N Grand Ave** where he observed DAGOSTINI enter the building carrying a black satchel and a shopping bag. The agent then entered the building and walked down the second floor common hallway past suite

[5] This is an address is the same address used in connection with identifiers for the synthetic identity of *Steven Dagostini* as further described below.

201. The office door was partially open and the agent observed DAGOSTINI sitting at a desk facing toward the door, working on a laptop computer. Later, the agent, who had resumed his surveillance outside the building, observed DAGOSTINI leave the building with the black satchel.

33. On July 6, 2020, a CPB officer assigned to the Milwaukee CBP office made a third seizure of counterfeit documents. He selected DHL international parcel 5829128384 for examination. The shipment was sent from Guangzhou Miaoyeguang Trading Company LTD of China to *Rudy PETERSON* at 238 Union Street, Waukesha, WI 53188 (**"238 Union Street"**) and was declared as "synthetic hair." The parcel contained a wig and three sets of counterfeit identity documents (six total). Again, the documents were counterfeit Wisconsin driver's licenses. One set contained the name *Riley CROSS*, DL number C620-7206-9291-01, DOB 08/11/1969, and address **311 N Greenfield Ave**; one set contained the name *Mark LONG*, DL number L502-5407-2292-03, DOB 08/12/1975, and address **511 E North Street, #129**. Both sets bore a picture of DAGOSTINI. The third set contained the name *Sophia DAGOSTINI,* DL number D223-7809-9622-03, DOB 04/02/1999, address **311 N Greenfield Ave**, and a picture of a young female. WIDOT has no record of issuing the Wisconsin driver's licenses with these numbers in the names *Riley CROSS* and *Mark LONG* and no record of issuing a driver's license with the number D223-7809-9622-03 in the name of *Sophia DAGOSTINI*. The documents were seized pursuant to Title 19, United States Code, Section 1595a(a), merchandise imported contrary to law, and Section 1584, false manifest. Further information about these synthetic identities is discussed in paragraphs herein. Copies of the counterfeit documents are set forth below.





34. I have determined that Sophia Dagostini is the daughter of DAGOSTINI and Sandra Randall. While WIDOT has no record of a Wisconsin Driver's License issued to Sophia Dagostini under the number on the seized driver's license, WIDOT does have a record that Sophia Dagostini of 311 N Greenfield Ave, Waukesha WI. 53186 was issued a Wisconsin Driver's license under a DL # D223-7840-1622-08 on August 4, 2017.

35. Waukesha County property tax records reflect that **238 Union Street**, Waukesha, WI, to which the seized package was addressed, is a residential property owned by Carl Ed and Debra L Cole. It is located adjacent to and just east of the **511 E North St** North Shore Station building that houses the MailEx service. The properties appear to be related as evidenced by a cable, possibly for surveillance cameras, which runs between and is connected to both buildings.

36. During law enforcement surveillance on October 15, 2020 at 10:21 a.m., DAGOSTINI was observed arriving at the parking lot adjacent to **511 E North St** in the black Mercedes Benz. He entered the building at the entrance closest to the MailEx service and remained

inside for approximately one minute. After appearing to place something in his vehicle, he walked toward **238 Union Street** and up to the northwest door where someone standing inside the building handed him an item that appeared to be mail matter. DAGOSTINI then returned to his vehicle and left the area.

The Current Investigation: Financial Information

37. Financial records and documents I have obtained during this investigation to date contain evidence that even before these counterfeit identity documents were seized in March, April, and July 2020, DAGOSTINI had opened checking and credit card accounts at multiple financial institutions using at least sixteen synthetic identities. Based on the dates that some of these accounts were established, it appears that this new fraudulent activity began while DAGOSTINI was on supervised release following his conviction. The following paragraphs summarize the account activity involving four suspected synthetic identities initially flagged by fraud investigators at Landmark Credit Union based on overlapping identifiers that tied to DAGOSTINI's own accounts at Landmark, as well as evidence I uncovered as I investigated the transactions in the Landmark records.

38. ***Sandy RANDALL***. Landmark credit card account x2790 was opened online on 10/22/2015. The application includes DAGOSTINI's ex-wife Sandra Randall's actual DOB and driver's license number; SSN 539-53-2209; a MailEx address **511 E North Street, #133** (the application lists the box number as Apt. 133) and DAGOSTINI's telephone number of **414 940-9975**. The application was generated from computer IP address **173.89.22.198**, which is administered by Charter Communications, and which has generated other fraudulent account applications linked to DAGOSTINI. The *Sandy RANDALL* Landmark account is linked to the email address **sandyis12345@gmail.com** which Google records show was opened on May 29,

2014 and registered to *Sandy RANDALL* with a recovery email address of **leedago@gmail.com** and a recovery phone number **414 940-9975**. The credit card account shows large dollar transactions, reversals, and since October 2016, a delinquent balance of $8,030.50.

39. Landmark Credit Union also provided me with copies of recorded telephone calls from a person identifying himself as *Sandy RANDALL*. USAO FLU Agent Kim Camomilli, who is familiar with DAGOSTINI's voice, listened to these calls and identified the caller as DAGOSTINI. Camomilli also provided me with a copy of a recorded voice mail message that DAGOSTINI left at her office. I have listened to that recording and compared it with the Landmark recordings. Based on that comparison I, too, believe that the Landmark calls were made by DAGOSTINI.

40. Other financial records I obtained in this investigation reflect that between 2015 and the present, checking, savings and/or credit card accounts were opened in the name *Sandy RANDALL* at Summit Credit Union, UW Credit Union, Barclays Bank, Discover, Wells Fargo, Elan, Bank of America, and Citibank using the same identifiers. Deposits into the *Sandy RANDALL* Summit checking and savings accounts include paychecks to, and direct deposits for, DAGOSTINI by Milwaukee Careers Cooperative, checks drawn on accounts in the name *Steven DAGOSTINI*, and cash advances from the *Sandy RANDALL* credit card account. There were also balance transfers, cash advances, and checks drawn on accounts at various other institutions in the names of *Anthony CAIRO, Patrick FRANKE, Frankie LANE, James PERRY, Jamie COOPER, Jay CASTRO* and *Mark LONG*. Funds from the Landmark checking account totaling more than $100,000 have made payments on an auto loan and other credit card accounts.

41. The following chart illustrates overlapping identifiers in the various *Sandy RANDALL* accounts, specifically, DAGOSTINI's phone number, **414 940-9975**, and the North Station MailEx address **511 E North St, #133**:

Institution	Account	Type	Balance	Address	Phone	Email
Landmark Credit Union	5755810	Checking		511 E North St #133	414-940-9975	sandyis12345@gmail.com
Landmark Credit Union	x2760	Credit	8,030.25	511 E North St #133	414-940-9975	sandyis12345@gmail.com
UW Credit Union	x2705	Credit	5,379.99	511 E North St #133	414-940-9975	sandyis12345@gmail.com
Barclay	x0801	Credit		511 E North St #133	414-940-9975	sandyis12345@gmail.com
Discover	x4026	Credit	$0	511 E North St #133	262-345-4163	sandyis12345@gmail.com
Discover	x6263	Credit	$0.00	5712 San Dell Wy, Racine, WI	424-940-9975	
Discover	x7976	Credit	$0	511 E North St	262-345-4163	sandyis12345@gmail.com
Summit Credit Union	x4300	Savings	1,805.27	511 E North St #133	414-651-2425	
Summit Credit Union	x0040	Checing	970.30		414-651-2425	
Summit Credit Union	x1969	Credit	22,200.00	511 E North St #133		
Summit Credit Union	x0001	Auto				
Wells Fargo	x5858	Credit	18,408.32	511 E North St #133		
Elan	x4933	Credit	5,688.50	511 E North St #133		
Bank of America	x9730	Credit	5,920.33	511 E North St #133	414-940-9975	
Citibank	x9107	Credit	10,471.51	511 E North St #133		

42. ***Herminio CASTRO***. Landmark checking account (x0002) and savings account (x0001) were opened online on 11/6/2015, also from IP address **173.89.22.198.** The application contains DOB 8/22/1979; SSN 348-04-8622; Wisconsin driver's license number C534-7936-6823-04 (of which WIDOT has no record); the MailEx address **511 E North St, #142,** Waukesha, WI; telephone number 262-347-4263; and email account **Hc2at12345@gmail.com**. The email account was created on March 1, 2015 also from the Charter Communications administered IP **173.89.22.198**, and was registered in the name *Herminio CASTRO*, with a recovery email **patis12345@gmail.com.** On 12/23/2016, the phone number on the account was updated to **414 940-9975**. The Landmark records show deposits of checks drawn on the accounts of *Mark LONG,* at Barclays and Wells Fargo, *Jamie COOPER* at Citi Bank, *Sandy RANDALL* at Summit Credit Union, *Chris MARKS* at Capital One and Ally, *Steven DAGOSTINI* at UW Credit Union, and *Frankie LANE* at Navy Federal Credit Union. The records also show deposits of checks written to other payees including *Anthony CAIRO*, *Pat FRANKE*, *Chris MARKS,* and *Jamie COOPER*. By September 13, 2019, the Landmark account balance had grown to $12,492.78. Payments from the

account went to various credit card companies including CitiCard, Discover, TD Bank, GTE Federal Credit Union, Wells Fargo, BMO Harris, Fifth Third Bank, and Capital One and to Vumber, (a business that provides virtual business phone numbers), and Virtualpostmail, (a mail service in California). Log-ins to the *CASTRO* Landmark accounts in March, April, May and June 2020 originated from IP **99.20.253.51**, which is an IP address administered by AT&T, and according to AT&T records, is assigned to Sandra Randall at **311 N Greenfield** Ave, Waukesha, WI.

43. On May 6, 2020, Landmark received a faxed letter with the return address **511 E North St, #129**, Waukesha, WI, requesting closure of the *CASTRO* accounts. Landmark refused to release the funds because the accounts lack signature cards or other proof of identity and the address **511 E North St, #129** differs from the address on the account application (**511 E North St, #142)**. As of May 2020, there was a checking balance of $3,886.56.

44**.** Landmark also provided me with recorded calls from a person identifying himself as *Herminio CASTRO*. Again, FLU Agent Camomilli and I both listened to the calls and recognized the voice as that of DAGOSTINI.

45. Other financial records I have reviewed during the course of this investigation reflect that between 2015 and the present, accounts have been opened in the name *Herminio_CASTRO* at Bank of America, Discover, Synchrony, Barclays, First National Bank of Omaha, Google Pay, and PayPal (P2P) using the same identifiers. The Google Pay account is associated with email **12zzaa567@gmail.com** and the PayPal account lists an associated business of HC Enterprises with multiple addresses including **311 N Greenfield Ave, 511 E North St**, **511 North E St #142,** and **340 Lemon Ave**, Walnut CA 91789.[6] The PayPal account is also linked to *CASTRO* accounts

[6] This address, 340 Lemon Ave, was also provided as an address change on an account in the name of *Frankie LANE* as further reflected below.

at Discover, Synchrony, Barclays, and First National Bank of Omaha. Email **castro.hermino@gmail.com** was linked to Discover and Barclays accounts.

46. The following chart illustrates overlapping identifiers in the various *Herminio CASTRO* accounts, specifically, DAGOSTINI's phone number, **414 940-9975**, DAGOSTINI's address, **311 N Greenfield Ave**, and the MailEx addresses **511 E North St, #133** and #**142**. Additionally, **9949 W. Atlantic Blvd**. is the Coral Springs, Florida address attributed to *Patrick FRANKE*, as principal of Plac Associates on the lease for **741 Grand Avenue**, **#201**, Waukesha, WI. (See paragraph 31 above.)

Institution	Account	Type	Balance	Address	Phone	Email
Landmark Credit Union	576488002	Checking	$3,886.56	511 E North St #142	262-347-4163	hc2at12345@gmail.com
Landmark Credit Union	5764880001	Savings	$5	511 E North St #142	414-940-9975	hc2at12345@gmail.com
Discover Bank	x7600	Credit	$4,651.81	311 N Greenfield Ave	414-940-9975	castro.hermno@gmail.com
Synchrony	x6457	Credit		311 N Greenfield Ave	414-940-9975	12zzaa567@gmail.com
Barclays	x7082	Credit	5,945	311 N Greenfield Ave	414-940-9975	castro.hermino@gmail.com
Bank of America	x8935	Credit	$2,478.00	311 N Greenfield Ave		
Bank of America	x1709	Checking	$91.57	9949 W Atlantic Blvd		
First National Bank of Omaha	x1080	Credit	$19,214.40	311 N Greenfield Ave		
First National Bank of Omaha	x2710	Credit				
Google Pay	12zzaa567@gmail.com					12zzaa567@gmail.com
PayPal	1701476752404822391	P2P		311 N Greenfield Ave		12zzaa567@gmail.com
				511 E North St #133		
				511 E North St #142		
				511 E North St		
				340 S Lemon Ave		

47. ***Steven DAGOSTINI***. Landmark account x1736 (later changed to x3636) was opened online in the name *Steven DAGOSTINI* on 11/16/2015. (Steven is DAGOSTINI's middle name.) The application contained DAGOSTINI's actual DOB 8/14/59, unique SSN, the MailEx address **511 E North St., #133**, DAGOSTINI's phone number **414 940-9975**, and DAGOSTINI's email address **leedago@gmail.com.** On 12/3/2015, the address for the Landmark account was updated to **N51W34917 Wis. Ave, #8, Okauchee, WI,** and the email updated to **stevenis1234@gmail.com.**

48. **N51W34917 Wisconsin Ave, Okauchee,**[7] **Wisconsin** ("**N51W34917 Wisconsin Ave**") is a multi-use property with commercial units on the main level and residential units on the upper level. The property has a parking lot to the rear, which is south of the building and accessible by Elm Avenue. The upper level is accessed by front and rear stairways that each have exterior doors. Waukesha County property records reflect that this property has been owned by WA Investments since approximately 2010. WE Energies records show several customers in this multi-use building. There are no WE energy records for *Steven DAGOSTINI* or for unit 8.

49. Mailboxes for the units at **N51W34917 Wisconsin Ave** are located on posts on Elm Avenue, which is located southeast of the building. Most of the mailboxes are labeled with numeric decals. One mailbox has a handwritten posting, stating that the box will accept mail for units 4, 5, 8 and 9. The doors on the upper level of the building have address numerals that correspond with numerals on the mailboxes. There are no doors bearing the numbers 4, 5, 8, or 9 nor does WE energy have records of service for any units with those numbers.

50. Google records reflect that the email address **stevenis1234@gmail.com** was created on May 31, 2014 and registered in the name *Steven DAGOSTINI,* with a recovery email **leedago@gmail.com.**

51. A review of the *Steven DAGOSTINI* Landmark credit card accounts reflect multiple charges at grocery stores, restaurants, a health center, and a convenience store. The May 2020 statement reflects a delinquent balance of $27,743.73.

52. Again, I listened to recorded calls provided by Landmark concerning account inquiries for the *Steven DAGOSTINI* account and have concluded that the calls were in fact placed by DAGOSTINI.

[7] N51W34917 Wisconsin Ave, Okauchee is also the purported principal business address on the Plac Associates lease (see paragraph 31 above.)

53. Other financial records I have received and reviewed for the synthetic identity *Steven DAGOSTINI* are from UW Credit Union (savings and credit card), Summit Credit Union (savings and credit card), Barclays (credit card), GTE Financial Credit Union (credit card), Discover (credit card), Synchrony Marvel (credit card), Bank of America (credit card), Wells Fargo (credit card), and Elan Financial (credit card). The activity in these accounts shows deposits of checks drawn on accounts in the names *Patrick FRANKE* and *Chris MARKS*, balances transfers between cards, cash withdrawals, and checks and cashier's checks with payees *Herminio CASTRO* and *Sandy RANDALL*. Most of the accounts currently have delinquent balances.

54. The following chart illustrates the overlapping identifiers in the various *Steven DAGOSTINI* accounts.

Institution	Account	Type	Balance	Address	Phone	Email
Landmark Credit Union	x1736 and x3636	Credit	$27,743.73	511 E North St #133	414-940-9975	leedago@gmail.com
UW CU	x2201	Savings		511 E North St #133	414-940-9975	stevenis1234@gmail.com
UW CU	x9061 and x4839	Credit	$4,759.00	511 E North St #133	414-940-9975	stevenis1234@gmail.com
Barclay	x7144	Credit		511 E North St #133	414-940-9975	stevenis1234@gmail.com
GTE FCU	denied	Credit	0.00	511 E North St #133	918-695-7841	stevenis1234@gmail.com
Discover	x9389	Credit	$0	511 E North St #133	414-940-9975	stevenis1234@gmail.com
Discover	x8132	Credit	$3,756.33	340 S Lemon Ave #2944		
Syncrony Marvel	x5293	Credit	$0.00	511 E North St #133	414-940-9975	stevenis1234@gmail.com
Syncrony Marvel	x0828	Credit	$3,220.19	511 E North St #133		
Summit Credit Union	x2721	Savings	$0	511 E North St #133	918-695-7841	stevenis1234@gmail.com
Summit Credit Union	x2723	Credit	$20,788.98	N51W34917 Wisconsin Ave		
Bank of America	x7359	Credit	$9,991.00	511 E North ST		
Wells Fargo	x4898	Credit	$971.90	511 E North St #133		
Wells Fargo	x2842	Credit	$11,363.00	N51W34917 Wisconsin Ave #8		
Elan Financial	x8366	Credit	$0.00	511 E North St #133		

55. ***Frankie LANE.*** Landmark credit card account x 7120 was opened online on 8/22/2017. The application includes the DOB 8/15/765, SSN 750-18-0042, and the address 9442 W Fond Du Lac Ave, Milwaukee, Wisconsin, and the telephone number 262-239-0958. Sandy Beauchanmp was listed as a relative. A counterfeit Wisconsin driver's license with license number L500-2307-529502 and a picture of DAGOSTINI was included as proof of identity.

The account is linked to email **flis12345a@gmail.com** which was created from IP **65.31.99.180** on 11/9/2016. The same IP address generated an application for a Discover credit card by DAGOSTINI on 12/15/2017, an application for a Synchrony Bank credit card for *Herminio CASTRO* on March 1, 2015, and created email accounts registered to *Rudy PETERSON* (**rpis12345a@gmail. com**) on 11/16/2016, and *Mark LONG* (**mlis12345a@gmail.com**) on 4/10/17. (The name *Mark LONG* is also on one set of counterfeit DL's seized by CBP on July 6, 2020). The linked email has a recovery email address of **elizabeth234@gmail.com.** That email is also the recovery email for several other synthetic identities identified in this fraud scheme, including *Pat FRANKE* and *Rudy PETERSON*. On January 30, 2018, *Frankie LANE's* address for the Landmark account was updated to **340 South Lemon Avenue**. This address is a variation of one of several addresses listed for HC Enterprises in connection with the PayPal account associated with *Herminio CASTRO*. See paragraph 45 above. The *Frankie LANE* Landmark credit card was used for transactions at Meijer, PayPal and various businesses in and around Waukesha. As of September 2018, it had a delinquent balance of $8,399.95.

56. During my examination of the transaction records for the *Frankie LANE* Landmark account, I was able to identify accounts that had been created at other financial institutions with this same synthetic identity information, including checking, savings and credit card accounts at Navy Federal Credit Union; savings and credit card accounts at Digital Federal Credit Union; and credit

card accounts with Wells Fargo and Discover. At this time, those credit accounts appear to have approximately $43,000 in delinquent balances. Emails **fralan1975@gmail.com** and **frankielane100@yahoo.com** were linked to Navy Federal Credit Union and Digital Federal Credit Union, respectively.

57. In examining the records from the other *Frankie LANE* accounts, I observed that checks drawn on the checking account at Navy Federal Credit Union had payees that included *Herminio CASTRO* and *Sandy RANDALL*, and that transactions involving funds in Digital Federal Credit Union credit card account were initiated through IP **65.31.99.180** and **173.89.20.228**, static IP addresses that are administered by Charter Communications. These IP addresses are the same IP addresses from which DAGOSTINI submitted applications for Discover credit cards in his own name, which frequently accessed the *CASTRO* PayPal account, and which created applications for credit at Synchrony Bank in other synthetic identities.

58. I have also listened to recorded telephone calls to the Navy Federal Credit Union by a customer identifying himself as *Frankie LANE,* and I have identified the voice as DAGOSTINI's.

59. Through my analysis of records from the various accounts in the names *Sandy RANDALL, Herminio CASTRO, Steven DAGOSTINI*, and *Frankie LANE*, I have identified other suspected synthetic identity accounts summarized as follows:

60. ***Jamie COOPER***. Records obtained from Citibank, Synchrony Bank, Fifth Third Bank, Discover and Wells Fargo reflect credit card accounts for *Jamie COOPER* with addresses of **9949 W. Atlantic Blvd** and/or **511 E North Street**. Synchrony and Discover card applications were submitted through IP **173.89.20.228**. Landmark CU records reflect balance transfers to the synthetic account of *Sandy RANDALL*. Recorded phone calls to Fifth Third from a person purporting to be *Jamie COOPER* is identified as DAGOSTINI. On June 8, 2020, a fellow agent

observed DAGOSTINI attempt a transaction at the Waukesha Associated Bank ATM. Subsequently obtained Associated Bank records showed the transaction to be an attempt to withdraw cash with a Fifth Third Bank credit card issued in name *Jamie COOPER*. Email linked to the *Jamie COOPER* accounts is **jcis12345a@gmail.com**.

61. ***Jay CASTRO***. Records obtained from Barclays, Elan, and Synchrony Bank reflect credit card accounts for *Jay CASTRO* with an address of **340 S. Lemon Ave #2944** and a telephone number **414 949-9975.** Landmark CU records reflect transfers from those accounts to the previously described synthetic account of *Sandy RANDALL*. Emails linked to the *Jay CASTRO* accounts are **jayis12345@gmail.com** and **jay7nyc@gmail.com** with a recovery account of **jay7nyc@hotmail.com.**

62. ***James PERRY***. Records obtained from Discover, Wells Fargo, First National Bank of Omaha and Elan reflect credit card accounts in the name of *James PERRY* with addresses of **N51W34917 Wisconsin Ave., #4** and/or **340 Lemon Ave. #2944**. Just as there is no unit 8 at **N51W34917 Wisconsin Ave**, there is no unit 4. There is only the single mailbox that purports to accept mail addressed to the non-existent units 4, 5, 8 and 9. (See paragraph 49). The application for the Discover account was submitted from IP address **65.31.99.180** and the email address linked to the Discover account was created from IP **173.89.22.198.** Landmark CU records reflect balance transfers to the synthetic account of *Sandy RANDALL*. The voice on recorded phone calls to Elan Financial purporting to be *James PERRY* is identified as DAGOSTINI. The March and April 2020 seizures by CBP contained counterfeit Wisconsin Driver's licenses bearing the name *James PERRY* and a photo of DAGOSTINI. The email linked to the *James PERRY* accounts is **Jpis12345a@gmail.com** with a recovery email of **chrisis12345c@gmail.com.**

63. ***Chris MARKS***. Records from Barclays, TD Bank, Wells Fargo, Bank of America, and Elan reflect credit card accounts in the name of *Chris MARKS*. The address on the accounts is **511 E North St, # 142**, and the telephone number for the Barclays account is **414 940-9975**. The records reflect balance transfers from the Bank of America account to the synthetic *Sandy RANDALL* account at Landmark. Charges on the other credit cards include those at the University of Wisconsin-Whitewater (where one of DAGOSTNI's daughters attends school) and various locations in Waukesha and Okauchee. The voice on recorded telephone calls to Elan Financial by a person identifying himself as *Chris MARKS* is that of DAGOSTINI. On July 17, 2017, Transunion Credit Bureau received a letter providing updated contact information for *Chris MARKS*. The letter included a copy of a Wisconsin Driver's license in the name *Chris MARKS*. It contained a photo of DAGOSTINI. Four of the twelve counterfeit Wisconsin driver's licenses seized by CBP in March and April 2020 were in the name of *Chris MARKS* but contained a photo DAGOSTINI. The email addresses linked to the *Chris MARKS* accounts are **cmis12345a@gmail.com,** created from IP **65.31.99.180,** and **chrisis12345c@gmail.com**. The recovery email for **cmis12345a@gmail.com** is **markj1234a@gmail.com,** and the recovery email for **chrisis12345c@gmail.com** is **Biztimenow@gmail.com.** The recovery phone number is **414 940-9975.**

64. ***Dylan YATES.*** The name *Dylan YATES* is on two sets of counterfeit Wisconsin Driver's licenses bearing DAGOSTINI's photo seized by CBP in March and April 2020. Records from various financial institutions reflect applications for credit accounts in the name *Dylan YATES* with addresses and telephone numbers similar to others used by DAGOSTINI. One of those is Discover, which received an application for *Dylan YATES* with the fake address **N51W34917 Wisconsin Ave., #4** from IP **173.89.20.228,** which is the same IP address that generated Synchrony and Discover card applications for the synthetic identity *Jamie COOPER*. The *YATES* application

was denied. The email account **dyis12345a@gmail.com,** associated with the Discover application, was created August 30, 1017 from IP **65.31.99.180,** which is also associated with DAGOSTINI. The recovery email is **rpis12345a@gmail.com** which was created on 11/16/2016, also from IP **65.31.99.180**, and registered to *Rudy PETERSON*.

65. ***Patrick FRANKE***. Records from BBVA, Synchrony Bank, Barclay and Elan reflect credit card accounts in the name of *Patrick FRANKE* with an address of **9949 W Atlantic Boulevard** (the address attributed to *FRANKE* as the principal of Plac Associates, see paragraph 31 above). The BBVA, Synchrony and Barclays records reflect that the phone number **414 940-9975** is associated with the accounts. An additional credit card account in the name of *Patrick FRANKE* at Bank of America shows *Patrick FRANKE* to have an address of **238 Union Street**, the residence adjacent to the North Shore Station MailEx location from which DAGOSTINI appeared to collect mail matter on October 15, 2020. (See paragraph 36). It is also the address on the package of counterfeit Wisconsin driver's licenses addressed to *Rudy PETERSON* that was seized by CBP in July 2020. The credit card applications for the *Patrick FRANKE* accounts were generated from IP addresses **65.31.99.180** and **99.20.253.51**. The email account linked to all of the *Patrick FRANKE* credit card accounts is **pfis12345a@gmail.com.** It was created on December 29, 2016 from IP **65.31.99.180** and registered to *Patrick FRANKE*. The recovery address is **elizabethis234@gmail.com.**

66. ***Anthony CAIRO***. Records from Synchrony Bank, Wells Fargo, Landmark CU Elan, TD Bank and CitiBank reflect credit applications in the name of *Anthony CAIRO*, using the addresses **N51W34917 Wisconsin Ave., #5, 340 Lemon Ave., 340 Lemon Ave #2944** and **340 Lemon Ave. #7232.** The application to CitiBank also includes the phone number **414 940-9975.**

Landmark records reflect balance transfers between *Anthony CAIRO* accounts and those in the name *Sandy RANDALL*. In September 2017 and May 2019, Transunion received letters updating account information for *Anthony CAIRO*. The letters included a copy of a Wisconsin Driver's license. The photo on the license was a picture of DAGOSTINI. The email account linked to Anthony CAIRO's credit card accounts is **acis12345a@gmail.com**.

67. ***Mark LONG***. Records from Barclays, Discover, Navy Federal Credit Union, Wells Fargo, TD Bank and CitiBank all reflect credit applications resulting in credit card accounts for *Mark LONG*, with an address of **511 E North St.** and **511 E North St, # 129.** As described above, the name *Mark LONG*, with an address of **511 E North St, # 129**, along with a photo of DAGOSTINI is on one of the sets of counterfeit Wisconsin Driver's Licenses seized by CBP in July 2020. The email address linked to the *Mark LONG* credit card accounts is **mlis12345a@gmail.com**. This email was created April 10, 2017 from IP **65.31.99.180**. The recovery address is **chrisis12345m@gmail.com.**

68. ***Riley CROSS***. Records from Barclays, Unify Credit Union, Bank of America, TD Bank and Synchrony Bank all reflect credit card accounts opened in 2018 and 2019 in the name *Riley CROSS* with an address of **311 N Greenfield Ave**. The Bank of America and TD accounts have been used for balance transfers and have a collective balance of approximately $12,000. The name *Riley CROSS* with the address **311 N Greenfield Ave** is on one set of counterfeit Wisconsin licenses with DAGOSTINI's photo in the package that was seized by CBP on July 6, 2020. The email linked to the Riley CROSS credit card accounts is **Rcis12345a@gmail.com.** It was created on September 27, 2017 from IP **65.31.99.180**. The recovery email and phone number are **flis12345a@gmail.com** and **414 940-9975**.

69. ***Rudy PETERSON***. Records from GTE Federal Credit Union, Elan, CitiBank and PayPal reflect account applications in the name *Rudy PETERSON* with an address of **340 S Lemon Ave** or **340 S Lemon Ave, # 7232.** The records further reflect that the address for the GTE account was updated to **238 Union Street** and that the account has been electronically accessed from IP **99.20.253.51** and **173.89.20.228.** The address **238 Union Street**, which is adjacent to the North Shore Station MailEx facility, was also on the package of counterfeit Wisconsin driver's licenses addressed to *Rudy PETERSON* seized by CBP on July 6, 2020. The account is linked to email **rpis12345a@gamail.com**. This account was created November 16, 2016 from IP **65.31.99.180** and has a recovery email **elizabethis234@gmail.com.** The voice on recorded calls to GTE Credit Union concerning the account is recognized as that of DAGOSTINI. The GTE and Elan accounts have a collective delinquent balance of approximately $9,000. One of the two PayPal accounts is associated with the business name Sandy's Boulevard and linked to the email **sandysboulevard@gmail.com.** This email was created on December 13, 2017 from IP **2600:1700:9071:430:51a:cd7a:b977:c21**a and is registered to Sandy's Boulevard. It has a recovery email of **rudypllc@gmail.com.** The other PayPal account is linked to a Bank of America checking account opened in the name *Herminio CASTRO*. The records show an email for this account as **rudypllc@gmail.com.** This email, created December 12, 2017, also from IP **2600:1700:9071:430:51a:cd7a:b977:c21a,** is registered to *Rudy PETERSON*, and has a recovery email of **jay7nyc@hotmail.com.**

70**.** ***Mark JOHNSON***. Records from Synchrony Bank and Elan reflect account applications for credit cards in the name *Mark JOHNSON* with the addresses **340 S Lemon Ave, # 2944** and **N51W34917 Wisconsin Ave, #4**. The Synchrony Bank account has a telephone number of **414 940-9975** and is linked to the email **markj1234a@gmail.com.** The Synchrony applications

were submitted from IP **65.31.99.180** and include the same California driver's license number (E 3173846) that was included on credit card applications for *Anthony CAIRO* and *Rudy PETERSON*. The California Department of Transportation has no record of issuing this driver's license number to individuals with any of these names. The Elan accounts have been used for balance transfers and for transactions at grocery stores, restaurants and other services in Waukesha and Okauchee, Wisconsin. They currently have a delinquent balance of approximately $31,000. The email **markj1234a@gmail.com.** was created June 8, 205 from IP **173.89.22.198** and is registered in the name *Mark JOHNSON*. The recovery email is **patis789@gmail.com** and the recovery phone number is **414 940-9975.**

BACKGROUND CONCERNING EMAIL

71. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

72. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including

whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

73. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

74. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate

who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

75. In general, an email that is received is stored in the subscriber's "mailbox" on a service provider's server until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on a server indefinitely. Even if the subscriber deletes the email, it may continue to be available on a server for a certain period of time.

76. Google LLC has been sent Request for Preservation of Records Letters pursuant to Title 18 USC § 2703(f) via Google LLC's Law Enforcement Request System. These letters requested Google LLC preserve, among other things, all stored communications, records, and other evidence regarding accounts previously mentioned. Google LLC has assigned reference numbers to these requests as follows: 3671466, 3739025, 3790803, 3807387, 3844571, and 3934099.

CONCLUSION

77. Based on my investigation to date, and given the significant connections between the aforementioned synthetic identities and Lee DAGOSTINI, I believe that there is probable cause to believe that DAGOSTINI has used computers, the internet, and email accounts to defraud Landmark Credit Union, Summit Credit Union, Wells Fargo Bank, Bank of America, Digital Federal Credit Union, Discover, Elan Financial, Fifth Third Bank, First Bank of Omaha, GTE Financial Credit Union, Navy Federal Credit Union, Synchrony Bank, TD Bank, Unify Financial Credit Union, UW Credit Union, Barclays, and Capital One Bank by providing fraudulent information to open financial accounts, which were used to receive, send, and withdraw money derived from financial fraud schemes.

78. Financial accounts have been fraudulently opened and used with direct association to DAGOSTINI with the use of his photograph and voice, common IP addresses, physical addresses, phone numbers, and email accounts. Additionally, the fraudulent use of the accounts have been used for services common to DAGOSTINI and near DAGOSTINI's residence.

79. I know from my training and experience that financial fraud schemes require detailed record keeping, with written or electronic notes, including identity information, account numbers, passwords, addresses, phone numbers, and e-mail addresses. Records reviewed in this investigation indicate that accounts were used strategically to raise credit limits and then make payment so as to build a positive credit history for each synthetic identity. I know from my training and experience that such records and information are often kept electronically and stored in residences, digital accounts, and vehicles.

80. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that evidence of these offenses, more fully described

in Attachment A of this Affidavit, are located with Google, Inc, Microsoft Corporation, and Oath Holdings, Inc. I respectfully request that this Court issue a search warrant for the authorizing the seizure and search of the items in Attachment A.

ATTACHMENT A

This warrant applies to information associated with the following account that is stored at premises owned, maintained, controlled, or operated by Microsoft Corporation, an email and electronic services provider headquartered at One Microsoft Way, Redmond, WA 98052.

Jay7nyc@hotmail.com

ATTACHMENT B

Property to be seized

I. Information to be disclosed by Google, LLC, Microsoft Corporation, and Oath Holdings, Inc. (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the accounts, commonly known as subscriber or registration information, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

b. The types of services utilized;

c. The contents of all emails associated with the accounts including stored or preserved copies of emails sent to and from the accounts, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and any attachments associated with emails;

d. The details of electronic devices used to access such services such as serial numbers and other unique device identification numbers;

e. GPS data or location information associated with mapping and directional programs that utilize the account

f. All other records or other information stored using the accounts, including address books, contact lists, calendar data, pictures and videos, and files; and

g. All records pertaining to communications between the Provider and any person(s) regarding the accounts, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government **14 DAYS** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. §§ 1028, 18 U.S.C. §§ 1343, 18 U.S.C. §§ 1344, 18 U.S.C. §§ 1956, violations involving Lee DAGOSTINI and others, including for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) Evidence of violations of fraud and related activity in connection with identification documents;

(b) Evidence of violations of fraud by wire, radio, or television;

(c) Evidence of violations of bank fraud;

(d) Evidence of laundering of monetary instruments;

(e) Evidence indicating how and when the email accounts were accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email accounts owners;

(f) Evidence indicating the email accounts owners' state of mind as it relates to the crime under investigation;

(g) The identity of the person(s) who created or used the account, including records that help reveal the whereabouts of such person(s).

(h) The identity of person(s) that communicate with the account about matters relating to previously described criminal violations, including records that help reveal the whereabouts of such person(s).